CLAIMS

1. Method for security verification of a message (Msg) transmitted and received in electronic form which:

- on the transmitting side comprises the steps of associating with the message for its subsequent security verification a univocal message identifier (ID_{Msg}) and an identifier (ID_{CR}) for checking the identity of the message owner with the checking identifier (ID_{CR}) being obtained by applying to the univocal message identifier (ID_{Msg}) a coding associated with the owner of the message to be transmitted, and
- on the receiving side for security verification of a received message (Msg) comprises the steps of:
  - verifying and signaling the fact of having or not having received a message previously with the same univocal message identifier (ID_{Msg}) associated,
  - applying a decoding associated with a supposed owner of the received message to the checking identifier of the owner (ID_{CR}) associated with the received message, and
  - ascertaining and signaling the agreement or not between the univocal message identifier (ID_{Msg}) associated with the received message and the result (ID_{DCR}) of said decoding of the checking username (ID_{CR}).

2. Method in accordance with claim 1 in which before transmission the univocal message identifier (ID_{Msg}) and the

identifier (ID_{CR}) for checking the identity of the message owner are assembled in a unique compound identifier (ID_T).

3. Method in accordance with claim 1 in which on the transmitting side at least the checking identifier (ID_{CR}) is assembled with the message and transmitted therewith.

4. Method in accordance with claim 3 in which the assembling takes place by inserting the message identifier (ID_{Msg}) in the message (Msg) and applying the coding to the result of the insertion.

5. Method in accordance with claim 1 in which on the transmitting side, with the message to be transmitted is also associated an owner identifier (ID_{owner}) and on the receiving side the decoding to be applied is selected from among a plurality of possible decodings on the basis of the owner identifier (ID_{owner}) associated with the received message.

6. Method in accordance with claim 1 in which the coding and decoding are keyed encryption and decryption operations.

7. Method in accordance with claim 3 in which encryption and decryption are the type with public/private key.

8. Method in accordance with claim 1 in which ascertainment of the agreement between univocal message identifier (ID_{Msg}) associated with the message received and the result of the decoding of the checking username (ID_{CR}) consists of verifying the sameness between said univocal message identifier (ID_{Msg}) and the result of the decoding of the checking username (ID_{CR}).

9. System for a safety verification of a message (Msg)

transmitted and received in electronic form and comprising:

- on the transmitting side:
  - a univocal message username generator (ID_{Msg}),
  - an encoding device which receives the message username (ID_{Msg}) produced by the generator and codifies it in accordance with a code associated with the owner of the message to be transmitted to obtain therefrom an identifier (ID_{CR}) for checking the identity of the message owner,
  - transmission means which associate with the message to be transmitted the checking identifier (ID_{CR}) and the univocal message identifier (ID_{Msg}) obtained,
- on the receiving side for security verification of a received message (Msg):
  - a control device which verifies and signals that the message identifier (ID_{Msg}) associated with the received message has or has not been received previously,
  - a decoding device which receives the owner checking identifier (ID_{CR}) associated with the received message and applies thereto a decoding associated with a supposed owner of the received message,
  - verification means which ascertain and signal the agreement or not of the univocal message identifier (ID_{Msg}) with the result of

the decoding of the checking username (ID_{CR}).

10. System in accordance with claim 8 characterized in that the encoding and decoding devices are keyed encryption and decryption devices.

11. System in accordance with claim 9 characterized in that the encryption and decryption devices are the public/private key type.

12. Device for association of security verification factors with a message transmitted in electronic form characterized in that it comprises:

- a univocal message username generator (ID_{Msg}),
- an encoding device which receives the message username (ID_{Msg}) produced by the generator and encodes it in accordance with a code associated with the owner of the message to be transmitted to obtain therefrom an identifier (ID_{CR}) for checking the identity of the message owner,
- means which associate with the message to be transmitted the checking identifier (ID_{CR}) and the univocal message identifier (ID_{Msg}) obtained.

13. Device in accordance with claim 12 characterized in that the encoding device is a keyed encryption device.

14. Device in accordance with claim 12 characterized in that it issues a compound identifier (ID_T) made up of the combination of the univocal message identifier (ID_{Msg}) and the identifier (ID_{CR}) for checking the identity of the message owner.